BAB I
PENDAHULUAN

A. Latar Belakang

Kemajuan dan perkembangan teknologi informasi dewasa ini telah berpengaruh pada seluruh aspek kehidupan manusia, termasuk bidang komunikasi. Pada saat yang sama keuntungan ini juga digunakan untuk melakukan tindakan ilegal misal peretasan informasi transaksi bank, username dan kata kunci. Mengingat betapa bahayanya dampak yang diberikan, sehingga perlu diterapkan prosedur keamanan pada informasi khususnya informasi berupa teks yang merupakan bentuk penting dari informasi digital. Informasi-informasi rahasia perlu disimpan atau disampaikan melalui suatu cara tertentu agar tidak diketahui oleh pihak lain yang tidak dikehendaki. Selanjutnya, untuk mengatasi permasalahan di atas, dapat diselesaikan dengan kriptografi.

Kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan pesan dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Dalam kriptografi dikenal dua penyandian, yakni enkripsi dan dekripsi. Enkripsi adalah sebuah proses penyandian yang mengubah sebuah kode pesan yang mudah dimengerti (*plaintext*) menjadi sebuah kode pesan yang tidak bisa dimengerti (*ciphertext*). Dekripsi adalah kebalikan dari enkripsi yaitu proses penyandian yang mengubah sebuah kode pesan yang tidak bisa dimengerti (*ciphertext*) menjadi kode pesan yang mudah dimengerti (*plaintext*). Ada beberapa teknik untuk mengubah (*plaintext*)

menjadi (*ciphertext*) atau (*ciphertext*) menjadi (*plaintext*). Teknik untuk mengubah (*plaintext*) menjadi (*ciphertext*) atau (*ciphertext*) menjadi (*plaintext*) dikenal sebagai algoritma (Munir, 2006).

Pada umumnya kriptografi dibedakan menjadi dua jenis yaitu kriptografi kunci simetris dan kriptografi kunci asimetris. Kriptografi kunci simetris merupakan kriptografi yang menggunakan kunci yang sama dalam proses enkripsi dan dekripsi. Contoh algoritma simetris adalah *Shift Cipher, Substitution Cipher, Affine Cipher*, *Hill Cipher*, dan *Vigenere Cipher*. Sedangkan kriptografi kunci asimetris yaitu kriptografi yang menggunakan dua kunci yang berbeda yaitu kunci publik dan kunci rahasia dalam proses enkripsi dan dekripsi. Kunci publik adalah kunci yang digunakan untuk proses enkripsi. Sedangkan kunci rahasia adalah kunci yang digunakan untuk mendekripsi informasi yang disandikan dengan tujuan mendapatkan informasi. Oleh karena itu kunci rahasia sebaiknya hanya diketahui oleh pendekripsi informasi yang disandikan. Contoh algoritma asimetris adalah RSA *(Rivest-Shamir-Adleman), ElGamal*, dan DSA *(Digital Signature Algorithm)* (Forouzan, 2007).

Berdasarkan artikel dalam suatu jurnal disimpulkan bahwa Penggabungan algoritma enkripsi *ElGamal* dan *Vigenere Cipher* adalah menggabungkan seni enkripsi modern dan klasik. Dengan menggunakan teknik ini, ketangguhan algoritma *ElGamal* akan semakin bertambah dengan adanya perlindungan ganda dengan menggunakan *Vigenere Cipher*. Menggabungkan algoritma *ElGamal* dan *Vigenere Cipher* menghasilkan

algoritma yang semakin kuat sehingga akan semakin menyulitkan penyadap yang tidak berhak yang ingin membaca pesan. (Kurniawan, 2012: hal. 5).

Berdasarkan artikel dalam Jurnal Informatika Mulawarman pada Juli 2012, Hamdani menyampaikan bahwa *Affine Cipher* merupakan salah satu algoritma simetris yang memiliki keamanan cukup baik seperti hal-nya *Vigenere Cipher*, dalam hal mengamankan pesan rahasia, dengan kelebihan menggunakan angka bilangan prima serta memiliki dua data masukan kunci. Algoritma *ElGamal* sendiri memiliki tingkat keamanan dalam pemecahan masalah logaritma diskret pada grup pergandaan bilangan bulat modulo prima. Selain tingkat keamanan pada pemecahan logaritma diskret, algoritma *ElGamal* memiliki kelebihan dalam menghasilkan *ciphertext* yang berbeda untuk *plaintext* yang sama pada proses enkripsi, tetapi ketika *ciphertext* didekripsi akan menghasilkan *plaintext* yang sama (Hamdani, 2012: hal. 5)

Pada skripsi ini dijelaskan bagaimana mengamankan pesan rahasia dengan mengimplementasikan perlindungan ganda, yaitu mengkombinasikan algoritma *Affine Cipher* dan *ElGamal* untuk pengamanan pesan rahasia.

B. Batasan Masalah

Dalam tugas akhir ini, penulis membatasi permasalahan pada algoritma *Affine Cipher* dan *ElGamal*, yaitu proses enkripsi dan dekripsi algoritma *Affine Cipher* dan *ElGamal*, dan bagaimana proses pembentukan kunci pada algoritma *ElGamal*. Kemudian pembahasan hanya mengacu pada konsep matematis yang melandasi metode tersebut, dan matlab digunakan sebagai alat bantu perhitungan.

C. Rumusan Masalah

Dari pembatasan masalah yang telah diuraikan diatas, berikut merupakan beberapa rumusan masalah dalam penulisan tugas akhir ini :

1. Bagaimana proses enkripsi dan dekripsi pada algoritma *Affine Cipher*?
2. Bagaimana proses enkripsi dan dekripsi pada algoritma *ElGamal*?
3. Bagaimana proses enkripsi dan dekripsi kombinasi algoritma *Affine Cipher* dan algoritma *ElGamal*?

D. Tujuan

Dari pembatasan masalah dan rumusan masalah yang telah diuraikan, berikut merupakan tujuan dari penulisan dari tugas akhir ini :

1. Menjelaskan proses enkripsi dan dekripsi pada algoritma *Affine Cipher*.
2. Menjelaskan proses enkripsi dan dekripsi pada algoritma *ElGamal*.
3. Menjelaskan proses enkripsi dan dekripsi kombinasi algoritma *Affine Cipher* dan algoritma *ElGamal*.

E. Manfaat

Dari tujuan yang telah diuraikan diatas, ada beberapa manfaat dari penulisan tugas akhir ini :

1. Bagi Mahasiswa

   Menambah pengetahuan tentang proses enkripsi dan dekripsi algoritma *Affine Cipher* dan algoritma *ElGamal*, dapat mengetahui hasil kombinasi algoritma *Affine Cipher* dan algoritma *ElGamal*.

2. Bagi Universitas

   Hasil penelitian ini diharapkan dapat menambah bahan referensi yang bermanfaat bagi Universitas negeri Yogyakarta, khususnya pada jurusan Pendidikan Matematika.

3. Bagi Pembaca

   Hasil penelitian ini diharapkan dapat digunakan sebagai penambah informasi mengenai kombinasi algoritma *Affine Cipher* dan algoritma *ElGamal*.